

Asymptotic behavior of growth functions of D0L-systems

Julien Cassaigne

Christian Mauduit

François Nicolas

September 12, 2009

Abstract

A *D0L-system* is a triple (A, σ, w) where A is a finite alphabet, σ is an endomorphism of the free monoid over A , and w is a word over A . The *D0L-sequence* generated by (A, σ, w) is the sequence of words $(w, \sigma(w), \sigma(\sigma(w)), \sigma(\sigma(\sigma(w))), \dots)$. The corresponding sequence of lengths, *i.e.*, the function mapping each integer $n \geq 0$ to $|\sigma^n(w)|$, is called the *growth function* of (A, σ, w) . In 1978, Salomaa and Soittola deduced the following result from their thorough study of the theory of rational power series: if the D0L-sequence generated by (A, σ, w) is not eventually the empty word then there exist an integer $\alpha \geq 0$ and a real number $\beta \geq 1$ such that $|\sigma^n(w)|$ behaves like $n^\alpha \beta^n$ as n tends to infinity. The aim of the present paper is to present a short, direct, elementary proof of this theorem.

1 Introduction

1.1 Notation

As usual, \mathbb{N} , \mathbb{R} and \mathbb{C} denote the semiring of natural integers, the field of real numbers, and the field of complex numbers, respectively. For every $a, b \in \mathbb{N}$, $[a, b]$ denotes the set of all integers n such that $a \leq n \leq b$. Let $f, g : \mathbb{N} \rightarrow \mathbb{C}$. We write $f(n) \preceq g(n)$ if there exists a real number $\lambda > 0$ such that $\{n \in \mathbb{N} : |f(n)| > \lambda |g(n)|\}$ is finite. We write $f(n) \asymp g(n)$ if both $f(n) \preceq g(n)$ and $g(n) \preceq f(n)$ hold.

A *word* is a finite string of symbols. Word concatenation is denoted multiplicatively. For every word w , the *length* of w is denoted $|w|$. The word of length zero is called the *empty word*. For every symbol a and every word w , $|w|_a$ denotes the number of occurrences of a in w .

An *alphabet* is a finite set of symbols. Let A be an alphabet. The set of all words over A is denoted A^* . A mapping $\sigma : A^* \rightarrow A^*$ is called a *morphism* if $\sigma(xy) = \sigma(x)\sigma(y)$ for every $x, y \in A^*$. Clearly, σ is completely determined by its restriction to A . For every $n \in \mathbb{N}$, σ^n denotes the n^{th} iterate of σ : for every $w \in A^*$, $\sigma^0(w) = w$, $\sigma^1(w) = \sigma(w)$, $\sigma^2(w) = \sigma(\sigma(w))$, $\sigma^3(w) = \sigma(\sigma(\sigma(w)))$, etc.

A *D0L-system* [5] is defined as a triple (A, σ, w) where A is an alphabet, σ is a morphism from A^* to itself, and w is a word over A . The *growth function* of the D0L-system (A, σ, w) is defined as the integer sequence $(|w|, |\sigma(w)|, |\sigma^2(w)|, |\sigma^3(w)|, \dots)$. For every *D0L-system* (A, σ, w) , either the sequence $(w, \sigma(w), \sigma^2(w), \sigma^3(w), \dots)$ is eventually periodic or $\lim_{n \rightarrow \infty} |\sigma^n(w)| = \infty$.

1.2 Contribution

The aim of the paper is to present a short, elementary proof of the following theorem.

Theorem 1. *Let (A, σ, w) be a D0L-system such that $\sigma^n(w)$ is a non-empty word for every $n \in \mathbb{N}$. There exist a non-negative integer α smaller than the cardinality of A , and a real number $\beta \geq 1$ such that $|\sigma^n(w)| \asymp n^\alpha \beta^n$ as $n \rightarrow \infty$.*

Theorem 1 plays a crucial role in the proof of an important result: Pansiot's theorem concerning the complexity of pure morphic sequences [7].

In 1978, Salomaa and Soittola laboriously proved a stronger result than Theorem 1.

Theorem 2 (Salomaa and Soittola [10, 1]). *Let (A, σ, w) be a D0L-system such that $\sigma^n(w)$ is a non-empty word for every $n \in \mathbb{N}$. There exist a positive integer q , a non-negative integer α smaller than the cardinality of A , and a real number $\beta \geq 1$ such that for each $r \in [0, q - 1]$,*

$$\frac{|\sigma^{nq+r}(w)|}{(nq+r)^\alpha \beta^{nq+r}}$$

converges to a positive, finite limit as $n \rightarrow \infty$.

The proof of Theorem 1 presented below cannot likely be refined into a proof of Theorem 2. The original proof of Theorem 2 relies on the theory of rational power series. In particular, two deep results are put to use:

1. Schützenberger's representation theorem [10, 1], and
2. Berstel's theorem concerning the minimum-modulus poles of univariate rational series over the semiring of non-negative real numbers [10, 1].

To conclude this section note that a very interesting particular case of Theorem 2 can be simply deduced from the Perron-Frobenius theory.

Definition 1 (Irreducibility and period). *Let A be an alphabet and let $\sigma : A^* \rightarrow A^*$ be a morphism. We say that σ is irreducible if for each $(a, b) \in A \times A$, there exists $k \in \mathbb{N}$ such that a occurs in $\sigma^k(b)$. For every $a \in A$, the period of a under σ is defined as the greatest common divisor of $\{k \in \mathbb{N} : |\sigma^k(a)|_a \neq 0\}$.*

If the morphism σ is irreducible then all letters in A have the same period under σ . If σ is irreducible and if every letter in A is of period one under σ then σ is called *primitive*: there exists $N \in \mathbb{N}$ such that for each $(a, b) \in A \times A$, a occurs in $\sigma^N(b)$.

Theorem 3 ([8]). *Let A be an alphabet, let $\sigma : A^* \rightarrow A^*$ be an irreducible morphism, and let q denote the period under σ of any letter in A . There exists a real number $\beta \geq 1$ such that for each $(a, b) \in A \times A$ and each $r \in [0, q - 1]$,*

$$\frac{|\sigma^{nq+r}(a)|_b}{\beta^{nq+r}}$$

converges to a positive, finite limit as $n \rightarrow \infty$.

2 Proof of Theorem 1

Our proof of Theorem 1 relies on the equivalence of norms on a finite-dimensional vector space (see Theorem 4 below). For the sake of completeness, the definition of a norm is recalled.

Definition 2 (Norm). *Let V be a real or complex vector space. A norm on V is a mapping $\|\cdot\|$ from V to \mathbb{R} such that the following three properties hold for all vectors $x, y \in V$ and all scalars $\lambda \in \mathbb{R}$:*

1. $\|x\| = 0$ if, and only if, x is the zero vector,
2. $\|\lambda x\| = |\lambda| \|x\|$, and
3. $\|x + y\| \leq \|x\| + \|y\|$.

Theorem 4 ([4, Corollary 3.14]). *Let V be a real or complex vector space. If the dimension of V is finite then for any norms $\|\cdot\|_A$ and $\|\cdot\|_B$ on V , there exist positive real numbers λ and μ such that $\lambda \|x\|_A \leq \|x\|_B \leq \mu \|x\|_A$ for every $x \in V$.*

Throughout this section d denotes a positive integer and $\mathbb{C}^{d \times d}$ denotes the algebra of d -by- d complex matrices. The following two classical norms on $\mathbb{C}^{d \times d}$ play a central role in our discussion.

Definition 3. *For every $X \in \mathbb{C}^{d \times d}$, define $\|X\|_1$ as the Manhattan norm of X : $\|X\|_1$ equals the sum of the magnitudes of the entries of X .*

Definition 4. *For every $X \in \mathbb{C}^{d \times d}$, define $\|X\|_\infty$ as the maximum norm of X : $\|X\|_\infty$ equals the maximum magnitude of the entries of X .*

It is clear that $\|X\|_\infty \leq \|X\|_1 \leq d^2 \|X\|_\infty$ for every $X \in \mathbb{C}^{d \times d}$.

The next proposition, which is mainly folklore, is the main ingredient of the proof of Theorem 1.

Proposition 1. *For each non-nilpotent matrix $M \in \mathbb{C}^{d \times d}$, there exist a norm $\|\cdot\|$ on $\mathbb{C}^{d \times d}$, an integer $\alpha \in [0, d - 1]$ and a real number $\beta > 0$ such that the ratio $\frac{\|M^n\|}{n^\alpha \beta^n}$ converges to a positive, finite limit as $n \rightarrow \infty$.*

Proof. Let $P \in \mathbb{C}^{d \times d}$ be a non-singular matrix such that $PM P^{-1}$ is in Jordan normal form: there exist $D, N \in \mathbb{C}^{d \times d}$ such that D is diagonal, N is nilpotent, $PM P^{-1} = D + N$ and $DN = ND$. Let $\|\cdot\|$ be the norm on $\mathbb{C}^{d \times d}$ defined by: $\|X\| := \|PXP^{-1}\|_\infty$ for every $X \in \mathbb{C}^{d \times d}$.

For all $i, j \in [1, d]$, let $e_{i,j} : \mathbb{N} \rightarrow \mathbb{C}$ be the function mapping each $n \in \mathbb{N}$ to the $(i, j)^{\text{th}}$ entry of $PM^n P^{-1}$. It is clear that $\|M^n\| = \max_{i,j \in [1,d]} |e_{i,j}(n)|$ for every $n \in \mathbb{N}$. Let I be the set of all $(i, j) \in [1, d] \times [1, d]$ such that $e_{i,j}$ is not eventually zero. Since M is not nilpotent, I is non-empty, and thus

$$\|M^n\| = \max_{(i,j) \in I} |e_{i,j}(n)|$$

for every sufficiently large $n \in \mathbb{N}$.

For each $n \in \mathbb{N}$, the binomial theorem yields:

$$PM^n P^{-1} = (D + N)^n = \sum_{k=0}^n \binom{n}{k} D^{n-k} N^k.$$

Besides, N^k is a zero matrix for every integer $k \geq d$, and thus

$$PM^n P^{-1} = \sum_{k=0}^{d-1} \binom{n}{k} D^{n-k} N^k$$

for every integer $n \geq d-1$. Hence, for each $(i, j) \in I$, there exist a non-zero eigenvalue λ_i of D and a non-zero complex polynomial $f_{i,j}$ with $\deg f_{i,j} \leq d-1$ such that

$$e_{i,j}(n) = f_{i,j}(n) \lambda_i^n$$

for every integer $n \geq d-1$:

Let (β, α) be the maximum element of $\{(|\lambda_i|, \deg f_{i,j}) : (i, j) \in I\}$ according to the lexicographical order. Let J denote the set of all $(i, j) \in I$ such that $(|\lambda_i|, \deg f_{i,j}) = (\beta, \alpha)$, and for each $(i, j) \in J$, let $c_{i,j}$ denote the leading coefficient of $f_{i,j}$. It is clear that

$$\lim_{n \rightarrow \infty} \frac{|e_{i,j}(n)|}{n^\alpha \beta^n} = \begin{cases} |c_{i,j}| & \text{if } (i, j) \in J \\ 0 & \text{otherwise} \end{cases}$$

for every $(i, j) \in I$, so

$$\lim_{n \rightarrow \infty} \frac{\|M^n\|}{n^\alpha \beta^n} = \max_{(i,j) \in I} \left(\lim_{n \rightarrow \infty} \frac{|e_{i,j}(n)|}{n^\alpha \beta^n} \right) = \max_{(i,j) \in J} |c_{i,j}|.$$

□

It follows from Theorem 4 that for any norms $\|\cdot\|_A$ and $\|\cdot\|_B$ on $\mathbb{C}^{d \times d}$ and for any $M \in \mathbb{C}^{d \times d}$, $\|M^n\|_A \asymp \|M^n\|_B$ as $n \rightarrow \infty$, so we get:

Corollary 1. *For each matrix $M \in \mathbb{C}^{d \times d}$, there exist an integer $\alpha \in [0, d-1]$ and a real number $\beta \geq 0$ such that for every norm $\|\cdot\|$ on $\mathbb{C}^{d \times d}$, $\|M^n\| \asymp n^\alpha \beta^n$ as $n \rightarrow \infty$.*

Proposition 1 deserves several comments. First, a more precise result is known.

Theorem 5 ([11, Theorem 3.1]). *Let $\|\cdot\|$ denote the spectral norm on $\mathbb{C}^{d \times d}$ and let $M \in \mathbb{C}^{d \times d}$ be such that M is not nilpotent.*

- *Let β denote the spectral radius of M .*
- *Let j denote the maximum size of the Jordan blocks of M with spectral radius β .*

The ratio $\frac{\|M^n\|}{n^{j-1}\beta^n}$ converges to a positive, finite limit as $n \rightarrow \infty$.

Let us also mention that a weak version of Theorem 5 holds in an arbitrary Banach algebra.

Theorem 6 (Gelfand's formula [9]). *Let \mathcal{A} be a complex Banach algebra and let $\|\cdot\|$ denote its norm. For every $M \in \mathcal{A}$, $\sqrt[n]{\|M^n\|}$ converges to the spectral radius of M as $n \rightarrow \infty$.*

Let us now illustrate Proposition 1 and Corollary 1 with an example. The matrix

$$M := \begin{bmatrix} 4 & -3 \\ 3 & 4 \end{bmatrix}$$

is diagonalizable:

$$PMP^{-1} = \begin{bmatrix} \lambda & 0 \\ 0 & \bar{\lambda} \end{bmatrix},$$

where i denotes the imaginary unit,

$$\lambda := 4 + 3i, \quad \bar{\lambda} := 4 - 3i, \quad P := \begin{bmatrix} 1 & i \\ 1 & -i \end{bmatrix} \quad \text{and} \quad P^{-1} := \frac{1}{2} \begin{bmatrix} 1 & 1 \\ -i & i \end{bmatrix}.$$

Let $\|\cdot\|$ be the norm on $\mathbb{C}^{2 \times 2}$ defined by: $\|X\| := \|PXP^{-1}\|_\infty$ for every $X \in \mathbb{C}^{2 \times 2}$. For every $n \in \mathbb{N}$, we have

$$M^n = P^{-1} \begin{bmatrix} \lambda^n & 0 \\ 0 & \bar{\lambda}^n \end{bmatrix} P = \frac{1}{2} \begin{bmatrix} \lambda^n + \bar{\lambda}^n & i\lambda^n - i\bar{\lambda}^n \\ -i\lambda^n + i\bar{\lambda}^n & \lambda^n + \bar{\lambda}^n \end{bmatrix} = 5^n \begin{bmatrix} \cos(n\theta) & -\sin(n\theta) \\ \sin(n\theta) & \cos(n\theta) \end{bmatrix},$$

where θ is an argument of λ ; so

$$\frac{\|M^n\|}{5^n} = 1, \quad 2 \leq \frac{\|M^n\|_1}{5^n} \leq 2\sqrt{2} \quad \text{and} \quad \frac{\sqrt{2}}{2} \leq \frac{\|M^n\|_\infty}{5^n} \leq 1.$$

Noteworthy is that no entry of $5^{-n}M^n$ converges as $n \rightarrow \infty$: both sets $\{\cos(n\theta) : n \in \mathbb{N}\}$ and $\{\sin(n\theta) : n \in \mathbb{N}\}$ are dense subsets of the closed real interval with endpoints -1 and $+1$ (see appendix).

We turn back to the proof of Theorem 1.

Lemma 1. *Let A be an alphabet, let $\sigma : A^* \rightarrow A^*$ be a morphism and let $w, x \in A^*$. If x occurs in $\sigma^{n_0}(w)$ for some $n_0 \in \mathbb{N}$ then $|\sigma^n(x)| \preceq |\sigma^n(w)|$ as $n \rightarrow \infty$.*

Proof. Let $L := \max_{a \in A} |\sigma^{n_0}(a)|$. If x occurs in $\sigma^{n_0}(w)$ then for every $n \in \mathbb{N}$, $\sigma^n(x)$ occurs in $\sigma^{n+n_0}(w)$, and thus

$$|\sigma^n(x)| \leq |\sigma^{n+n_0}(w)| = \sum_{a \in A} |\sigma^n(w)|_a |\sigma^{n_0}(a)| \leq L \sum_{a \in A} |\sigma^n(w)|_a = L |\sigma^n(w)|.$$

□

Definition 5. *A D0L-system (A, σ, w) is called reduced if for every $a \in A$ there exists $m \in \mathbb{N}$ such that a occurs in $\sigma^m(w)$.*

Lemma 2. *For any reduced D0L-system (A, σ, w) ,*

$$|\sigma^n(w)| \asymp \sum_{a \in A} |\sigma^n(a)| \tag{1}$$

as $n \rightarrow \infty$.

Proof. For every $n \in \mathbb{N}$, let

$$S_n := \sum_{a \in A} |\sigma^n(a)|.$$

First, we have

$$|\sigma^n(w)| = \sum_{a \in A} |w|_a |\sigma^n(a)| \leq \left(\max_{a \in A} |w|_a \right) S_n,$$

and thus $|\sigma^n(w)| \preceq S_n$. Conversely, Lemma 1 ensures $|\sigma^n(a)| \preceq |\sigma^n(w)|$ for each $a \in A$ because the D0L-system (A, σ, w) is reduced. It follows $S_n \preceq |\sigma^n(w)|$. □

Proof of Theorem 1. Let us first check that, without loss of generality, we may assume that (A, σ, w) is reduced. Let \bar{A} denote the set of all symbols $a \in A$ such that a occurs in $\sigma^m(w)$ for some $m \in \mathbb{N}$. Remark that $\sigma(\bar{A}) \subseteq \bar{A}^*$: for any $a \in \bar{A}$ and any $m \in \mathbb{N}$ such that a occurs in $\sigma^m(w)$, $\sigma(a)$ occurs in $\sigma^{m+1}(w)$, and thus $\sigma(a) \in \bar{A}^*$. Hence σ induces a morphism $\bar{\sigma} : \bar{A}^* \rightarrow \bar{A}^*$: $\bar{\sigma}(x) = \sigma(x)$ for every $x \in \bar{A}^*$. Clearly, $(\bar{A}, \bar{\sigma}, w)$ is a reduced D0L-system and $\sigma^n(w) = \bar{\sigma}^n(w)$ for every $n \in \mathbb{N}$. Therefore, we may replace (A, σ, w) with $(\bar{A}, \bar{\sigma}, w)$ in the remaining of the proof, so (1) holds by Lemma 2.

Let d denote the cardinality of A . Write arbitrarily A in the form $A = \{a_1, a_2, \dots, a_d\}$. Let M be the d -by- d matrix defined by: for all $i, j \in [1, d]$, the $(i, j)^{\text{th}}$ entry of M equals $|\sigma(a_j)|_{a_i}$. The $(i, j)^{\text{th}}$ entry of M^n equals $|\sigma^n(a_j)|_{a_i}$, and thus

$$\sum_{a \in A} |\sigma^n(a)| = \|M^n\|_1 \tag{2}$$

It follows from Corollary 1 that there exist an integer $\alpha \in [0, d-1]$ and a real number $\beta \geq 0$ such that

$$\|M^n\|_1 \asymp n^\alpha \beta^n \tag{3}$$

Combining (1), (2) and (3), we get $|\sigma^n(w)| \asymp n^\alpha \beta^n$. Since $|\sigma^n(w)| \geq 1$ for every $n \in \mathbb{N}$, $n^\alpha \beta^n$ does not converge to zero, and thus $\beta \geq 1$. □

References

- [1] J. Berstel and C. Reutenauer. *Rational series and their languages*, volume 12 of *EATCS Monographs on Theoretical Computer Science*. Springer-Verlag, 1988. The new version is presently available online at Berstel’s homepage.
- [2] G. H. Hardy and E. M. Wright. *An introduction to the theory of numbers*. Oxford, at the Clarendon Press, fourth edition, 1979.
- [3] I. Kaplansky. *Commutative rings*. The University of Chicago Press, revised edition, 1974.
- [4] S. Lang. *Real analysis*. Addison-Wesley Publishing Company, second edition, 1983.
- [5] A. Lindenmayer. Mathematical models for cellular interactions in development. *Journal of Theoretical Biology*, 18(3):280–315, 1968.
- [6] I. Niven and H. S. Zuckerman. *An introduction to the theory of numbers*. John Wiley and Sons, third edition, 1972.
- [7] J.-J. Pansiot. Complexité des facteurs des mots infinis engendrés par morphismes itérés. In *Proceedings of the 11th International Colloquium on Automata, Languages and Programming (ICALP’84)*, volume 172 of *Lecture Notes in Computer Science*, pages 380–389. Springer-Verlag, 1984.
- [8] M. Queffélec. *Substitution dynamical systems-spectral analysis*, volume 1294 of *Lecture Notes in Mathematics*. Springer-Verlag, 1987.
- [9] W. Rudin. *Functional analysis*. International Series in Pure and Applied Mathematics. McGraw-Hill, second edition, 1991.
- [10] A. Salomaa and M. Soittola. *Automata-theoretic aspects of formal power series*. Texts and Monographs in Computer Science. Springer-Verlag, 1978.
- [11] R. S. Varga. *Matrix iterative analysis*. Prentice-Hall, 1962.

Appendix

Throughout the section,

- π denotes Archimedes’ constant,
- $I := \{x \in \mathbb{R} : 0 \leq x \leq 1\}$, and
- $J := \{x \in \mathbb{R} : -1 \leq x \leq +1\}$.

The aim of this appendix is to prove the following proposition:

Proposition 2. *For any argument θ of $4 + 3i$, both sets $\{\cos(n\theta) : n \in \mathbb{N}\}$ and $\{\sin(n\theta) : n \in \mathbb{N}\}$ are dense subsets of J .*

Proposition 2 is a consequence of the following two well-known results.

Proposition 3 ([6, Theorem 6.15]). *Let ρ be a rational number. If $\cos(2\pi\rho)$ is rational then $2\cos(2\pi\rho)$ is an integer.*

Proof. Both complex numbers $\exp(2\pi\rho i)$ and $\exp(-2\pi\rho i)$ are algebraic integers. Indeed, they are roots of the monic integer polynomial $z^q - 1$, where q is a positive integer such that $q\rho$ is an integer. Since a sum of algebraic integers is also an algebraic integer [3, Theorem 13], $2\cos(2\pi\rho) = \exp(2\pi\rho i) + \exp(-2\pi\rho i)$ is an algebraic integer. If $\cos(2\pi\rho)$ is rational then $2\cos(2\pi\rho)$ is in fact an integer because an algebraic integer, if rational, is an integer [2, Theorem 206]. \square

Note that for any real number θ with $-\pi \leq \theta \leq \pi$, the following three assertions are equivalent:

1. $2\cos(\theta)$ is an integer,
2. $\cos(\theta) \in \{-1, -\frac{1}{2}, 0, +\frac{1}{2}, +1\}$, and
3. $|\theta| \in \{0, \frac{1}{3}\pi, \frac{1}{2}\pi, \frac{2}{3}\pi, \pi\}$.

Proposition 4 ([2, Theorem 439]). *For any irrational number $\rho \in \mathbb{R}$, $\{n\rho - \lfloor n\rho \rfloor : n \in \mathbb{N}\}$ is a dense subset of I .*

Proof of Proposition 2. Since the cosine of θ equals $\frac{4}{5}$, $\frac{\theta}{2\pi}$ is irrational by Proposition 3. Hence, $D := \{\frac{n\theta}{2\pi} - \lfloor \frac{n\theta}{2\pi} \rfloor : n \in \mathbb{N}\}$ is a dense subset of I by Proposition 4. Since the function $f : I \rightarrow J$ that maps each $x \in I$ to $\cos(2\pi x)$ is continuous and surjective, $\{\cos(n\theta) : n \in \mathbb{N}\} = f(D)$ is a dense subset of J . In the same way, the function $g : I \rightarrow J$ that maps each $x \in I$ to $\sin(2\pi x)$ is continuous, surjective and such that $\{\sin(n\theta) : n \in \mathbb{N}\} = g(D)$. \square